

# Diseño y simulación de un procesador cuántico

*Proyecto Informático*

---



escuela técnica superior  
de ingeniería informática



Jaime M<sup>a</sup> Coello de Portugal Vázquez

Dirigido por José Luis Guisado Lizar

**3 de Julio de 2013**

Ingeniería Informática

## 1

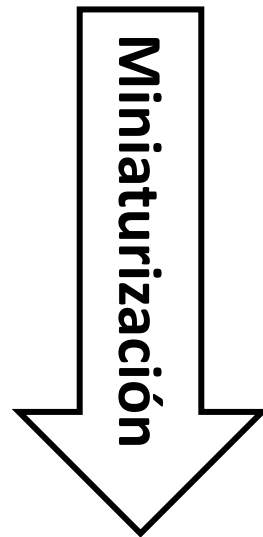
# Información cuántica

00110001	00001010	11010110	11001011	11011011	01011011	10101000	10001001
10000010	10111111					01100101	00010010
11011000	11100000					10100110	10000000
11101100	11010111					10010011	01000010
00011101	10000011	$H(t)  \psi(t)\rangle = i\hbar \frac{d}{dt}  \psi(t)\rangle$				00011100	11011111
10000100	11110101					10011110	00001111
11101010	10001010					00001001	11100000
00111000	01010001					00010011	01110000
00001011	00001101					10010111	01111011
		00101011	11001011	11010011	00010011		

# Información cuántica

*El ¿límite? en la miniaturización*

Física clásica



Física cuántica

Partículas bien definidas

Sistemas fácilmente observables

Estados robustos

Posición y velocidad

¿Partícula u onda?

Estados extremadamente frágiles

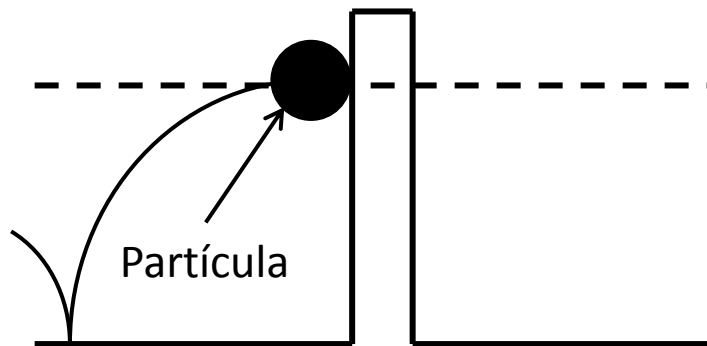
Observar un sistema lo modifica

Probabilidad

# Información cuántica

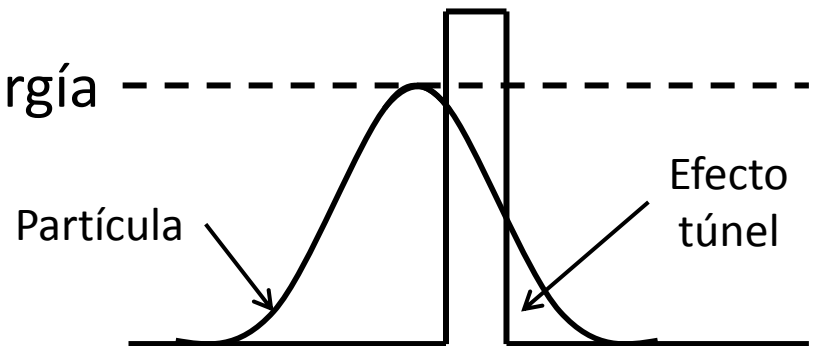
## *El efecto túnel*

### Física clásica



*Es **imposible** que la partícula supere la barrera*

### Física cuántica



*La partícula tiene una cierta **probabilidad** de superar la barrera*

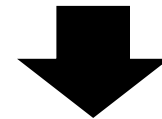
# Información cuántica

## *Inicios*

Los computadores son incapaces de imitar a la física cuántica eficientemente



Si fabricamos un ordenador que utilice la física cuántica podrá imitarla con facilidad



**Los computadores cuánticos serán superiores**



Richard Feynman

# Información cuántica

## *Ramas*

**Superposición de  
estados cuánticos**  
Computaciones más rápidas

### **Computación**

## **Cuánticas**

Teleportación

Criptografía

Envío rápido de información

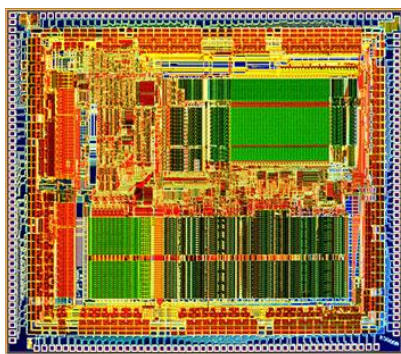
**Entrelazamiento  
cuántico**

Mensajes totalmente seguros

**Colapso de la función de  
onda**

# Información cuántica

## *El procesador clásico-cuántico*



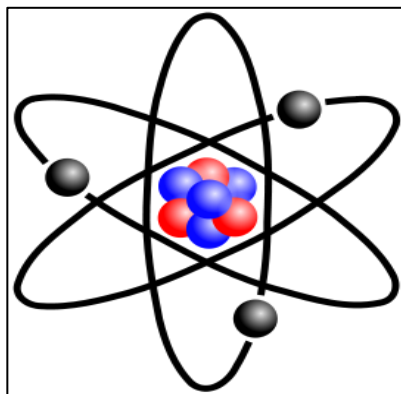
### Computador clásico

---

Muy general

Muy lento en algunos casos

Fácil de construir y manejar



Muy específico

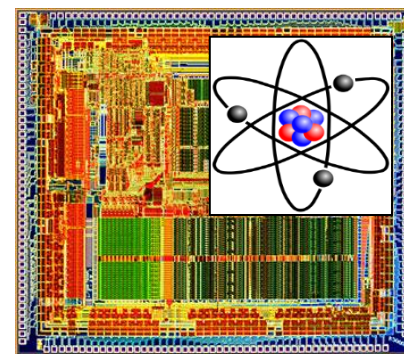
Muy rápido en algunos casos

Difícil de construir y manejar

### Computador cuántico

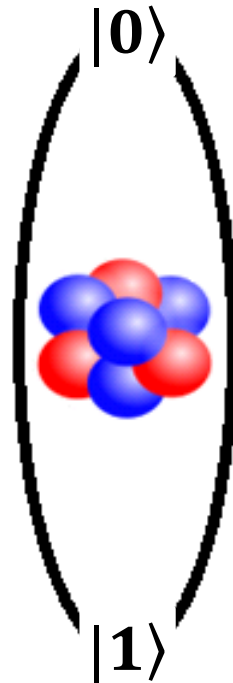
---

### Computador clásico-cuántico



# 2

## Computación cuántica





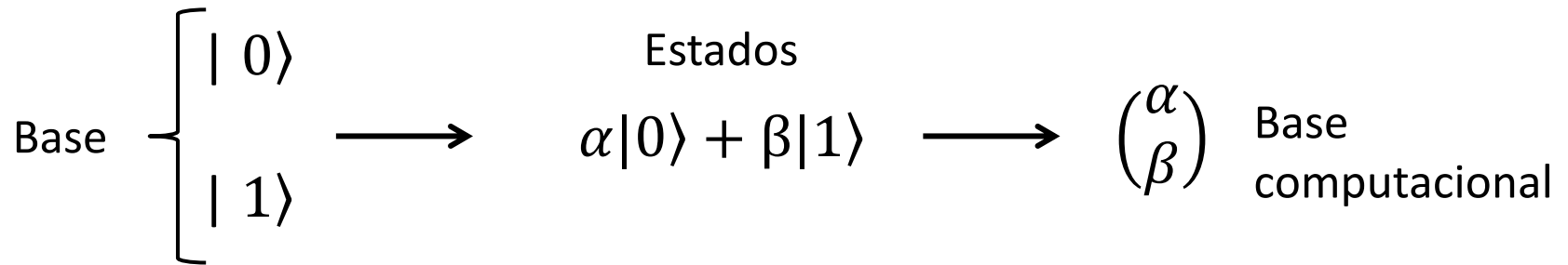
# Computación cuántica

## *El qubit*

El más simple de los espacios de estados

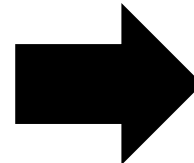
Dos dimensiones complejas

Quantum bit o qubit



$$\frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

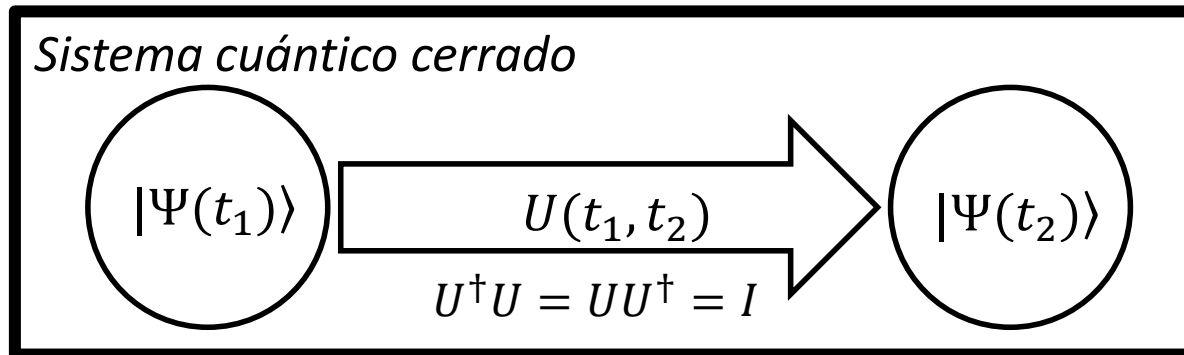
Es un estado válido



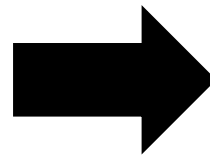
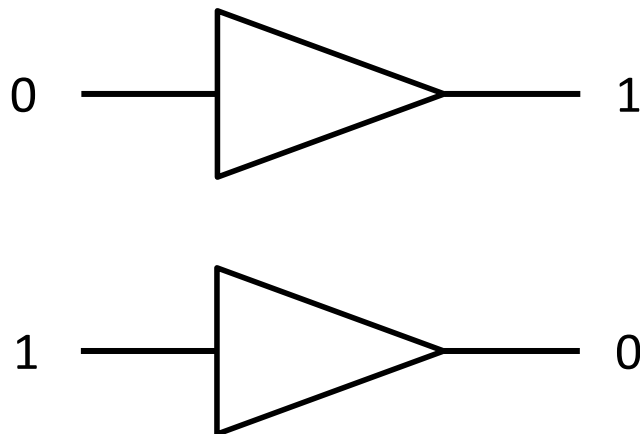
Paralelismo cuántico

# Computación cuántica

## *Las puertas cuánticas*



Puerta clásica: inversor lógico



Puerta cuántica: X

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

# Computación cuántica

## *Las puertas cuánticas*

### *Puertas de Pauli*

$$X|0\rangle = |1\rangle$$

$$X|1\rangle = |0\rangle$$

$$Y|0\rangle = i|1\rangle \quad Z|0\rangle = |0\rangle$$

$$Y|1\rangle = -i|0\rangle \quad Z|1\rangle = -|1\rangle$$

### *Cambio de fase*

$$P(\alpha)|0\rangle = |0\rangle$$

$$P(\alpha)|1\rangle = e^{i\alpha}|1\rangle$$

### *Puerta de Hadamard*

$$H|0\rangle = \frac{1}{\sqrt{2}}|0\rangle + \frac{1}{\sqrt{2}}|1\rangle$$

$$H|1\rangle = \frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle$$

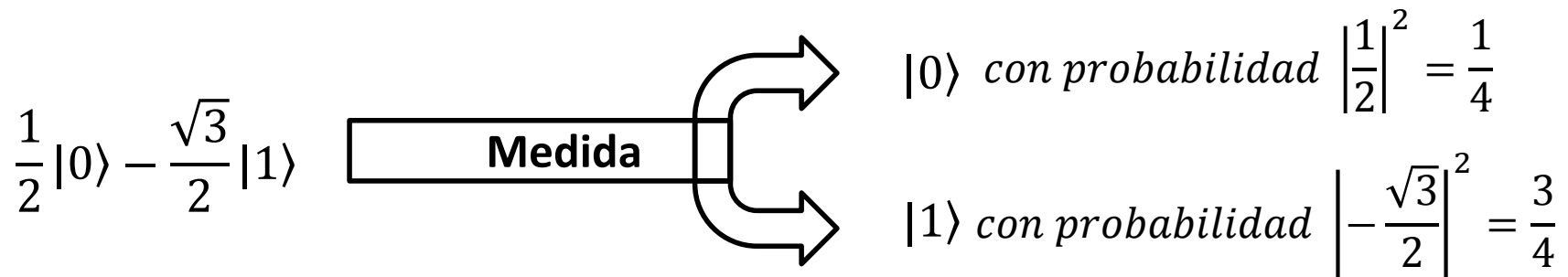
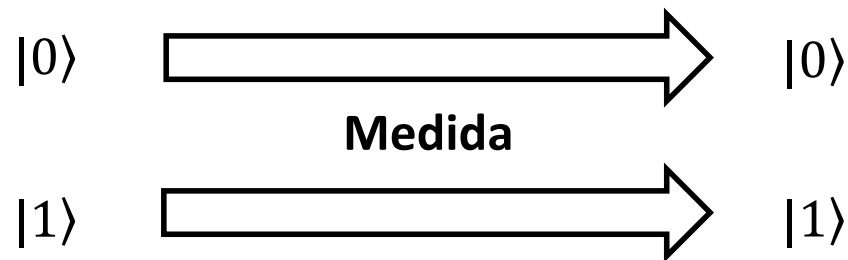
## **Paralelismo cuántico**

$$X(H|1\rangle) = X\left(\frac{1}{\sqrt{2}}|0\rangle - \frac{1}{\sqrt{2}}|1\rangle\right) = \frac{1}{\sqrt{2}}X|0\rangle - \frac{1}{\sqrt{2}}X|1\rangle$$

# Los postulados de la mecánica cuántica

## *Las medidas*

**El sistema deja de ser cerrado**



**La función de onda colapsa**

# Computación cuántica

## *Los sistemas multiqubit*

$$\left. \begin{array}{l} |\Psi\rangle \\ |\Phi\rangle \end{array} \right\} \text{ Combinados } \longrightarrow |\Psi\rangle \otimes |\Phi\rangle, \text{ o simplemente } |\Psi\Phi\rangle$$

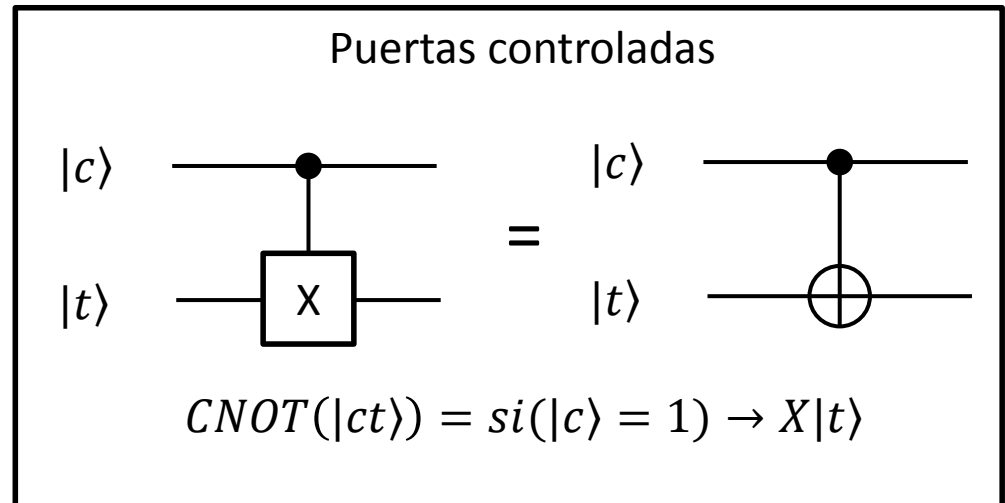
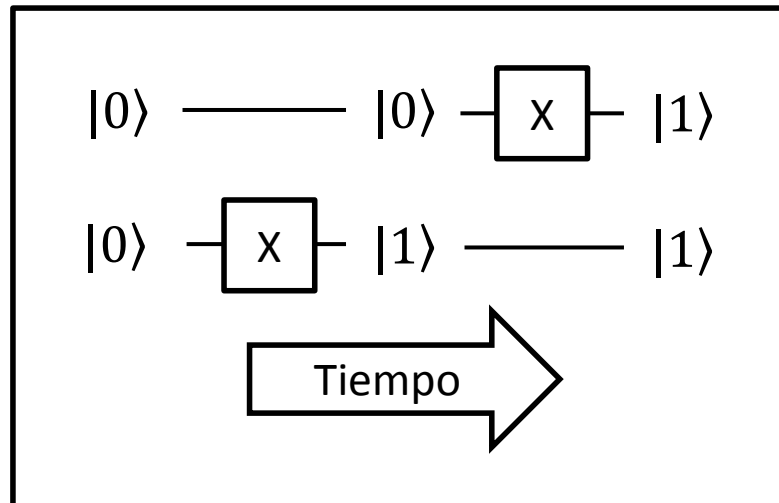
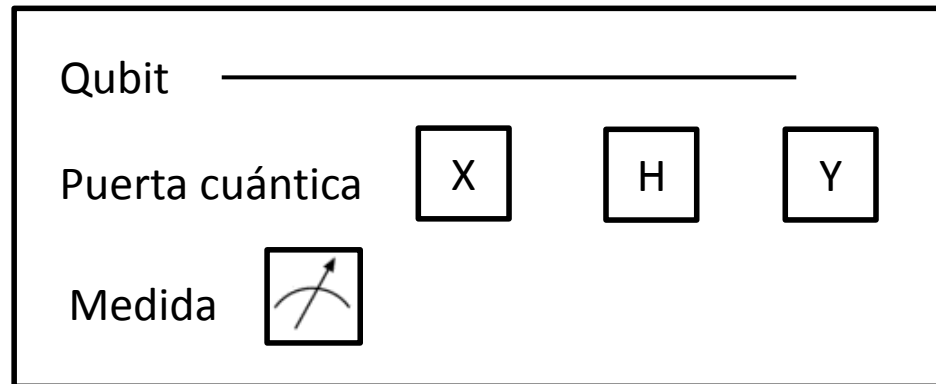
$$\text{Dos qubits } \alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$\text{Tres qubits } \alpha|000\rangle + \beta|001\rangle + \gamma|010\rangle + \delta|011\rangle + \dots$$

$$\text{Grados de libertad} \longrightarrow 2^{\text{número de qubits}}$$

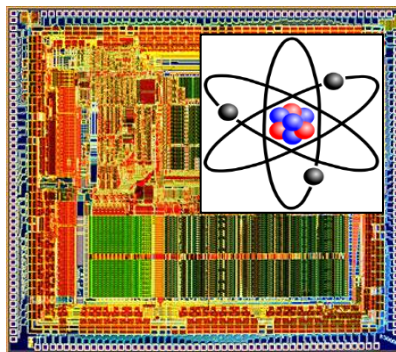
# Computación cuántica

## *Los circuitos cuánticos*



# 3

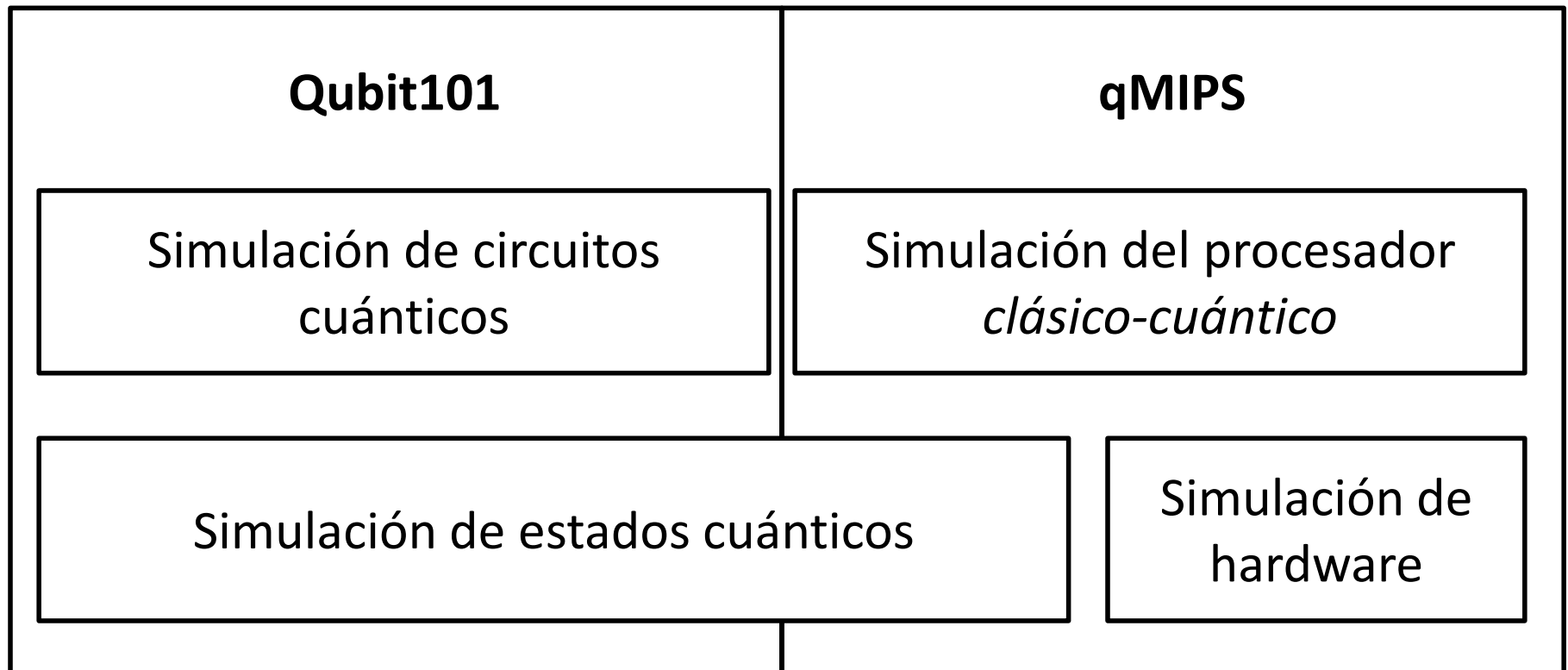
## Simulación



10000010100101  
10100101000101  
01010101010101  
0000101010100  
1010100010001010  
011111010100100100  
111110101010001010  
101010101010101010  
000001010000101011

# Simulación

## *Los simuladores*



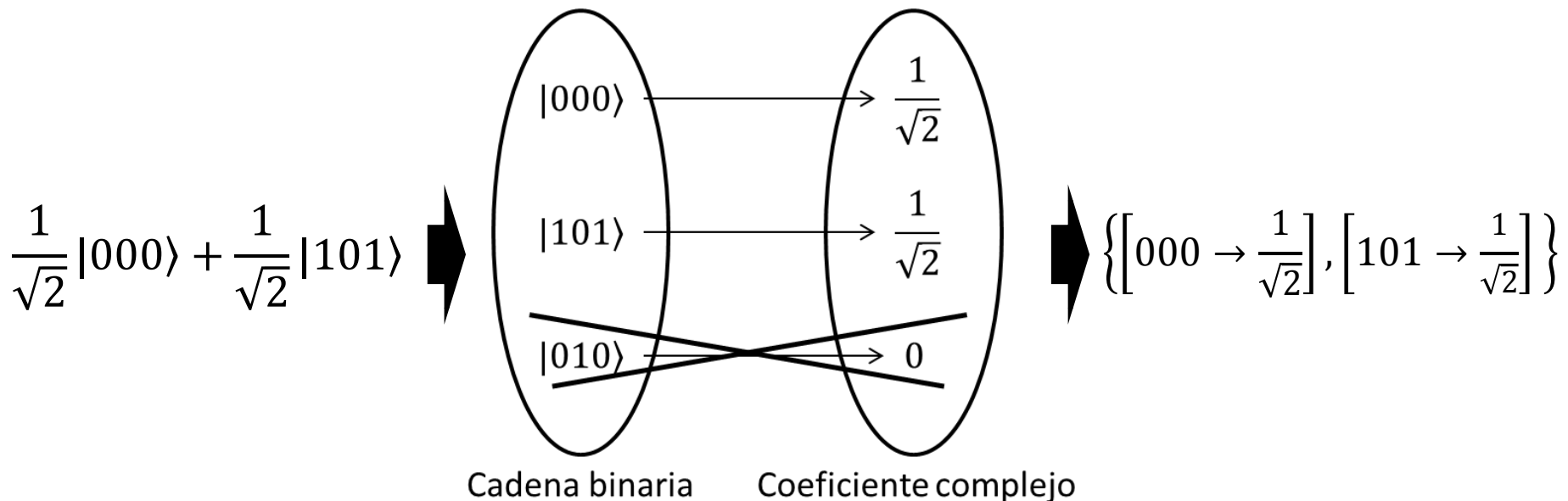


# Simulación

*Motor de simulación de estados cuánticos*

$$\alpha|00\rangle + \beta|01\rangle + \gamma|10\rangle + \delta|11\rangle$$

$$\{[00 \rightarrow \alpha], [01 \rightarrow \beta], [10 \rightarrow \gamma], [11 \rightarrow \delta]\}$$



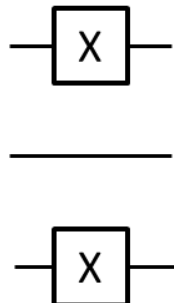
# Simulación

## *Motor de simulación de estados cuánticos*

Puerta  $P$  sobre  
qubit  $q$  del  
estado  $|\Psi\rangle$



Subrutina  $P(q, \Psi)$

$$(X \otimes I \otimes X)|000\rangle = |101\rangle \xrightarrow{\quad} |000\rangle \xrightarrow{\quad} |101\rangle$$




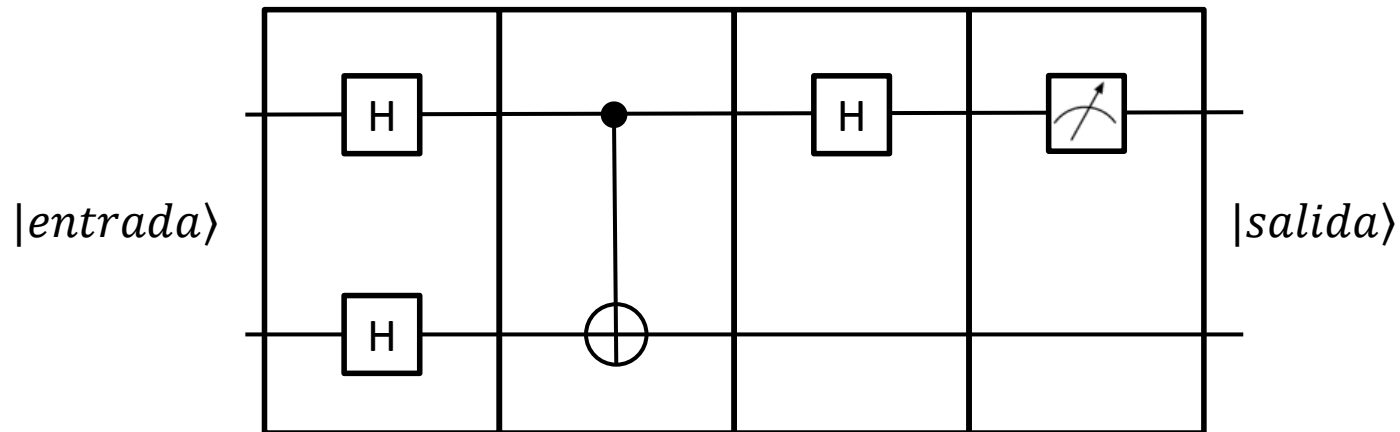
$$X(0, \{[000 \rightarrow 1]\}) \rightarrow \{[100 \rightarrow 1]\}$$

$$X(2, \{[100 \rightarrow 1]\}) \rightarrow \{[101 \rightarrow 1]\}$$


# Simulación


## *Motor de simulación de circuitos*

**Circuito** = *Array*{ Etapa 0 Etapa 1 Etapa 2 Etapa 3 }



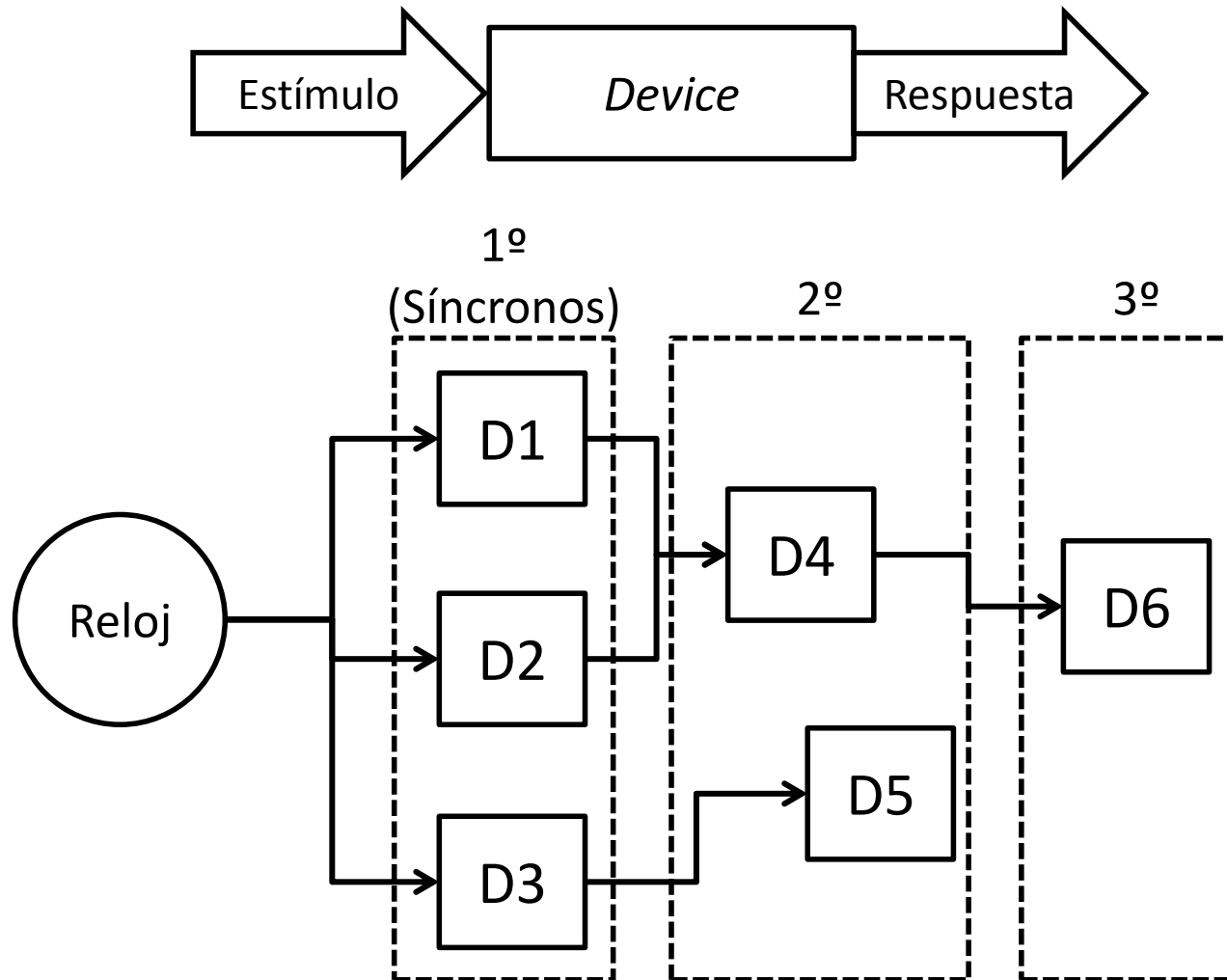
→ **Etapa** = *Array*

Puerta 0 —  —

Puerta 1 —  —

# Simulación

## *Motor de simulación de hardware*



4

# Arquitectura qMIPS



# Arquitectura qMIPS

## *La arquitectura MIPS*

**Arquitectura RISC estricta:** *Reduced Instruction Set Computing*

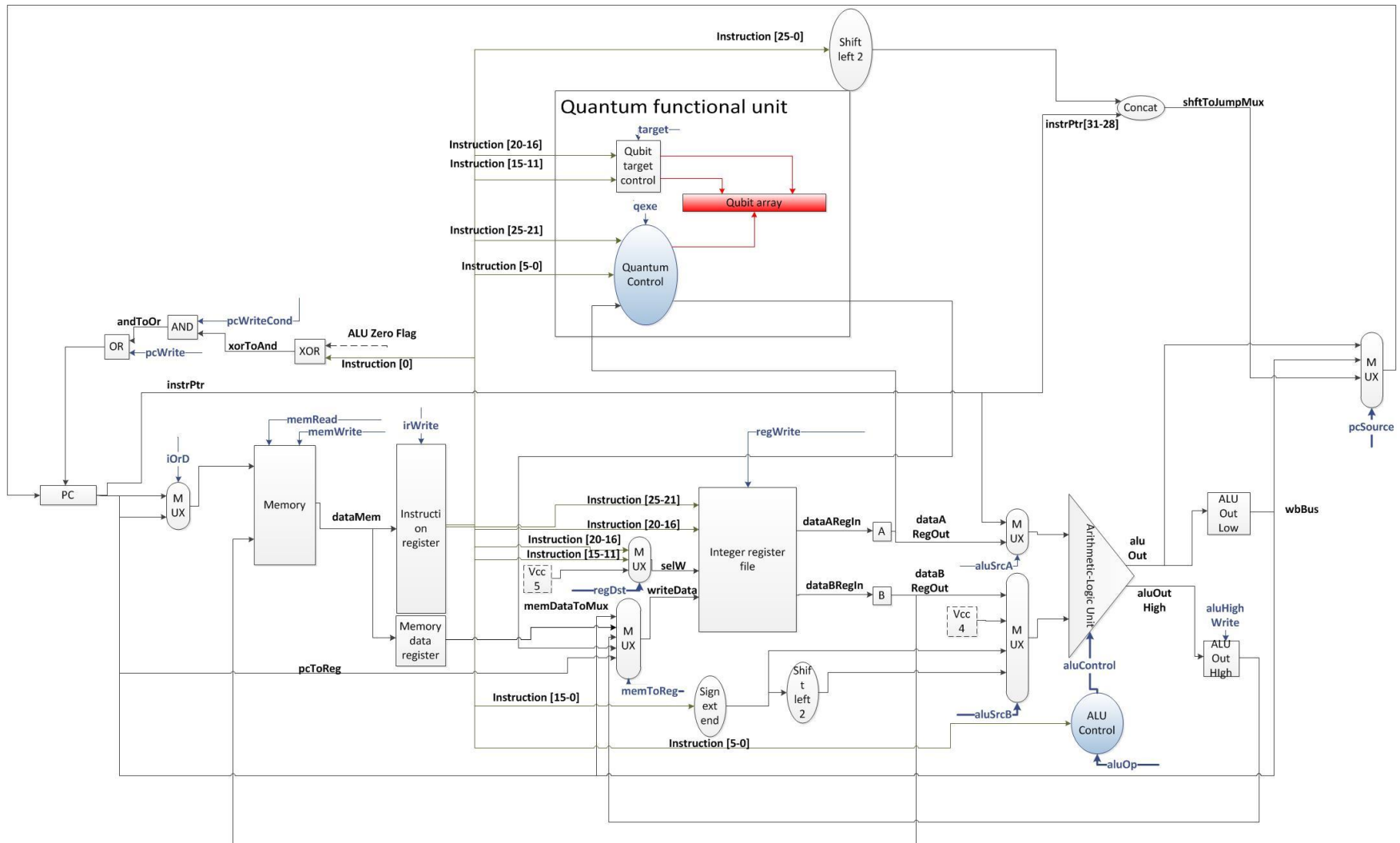
**Ejecución en cinco fases:** {

- IF: *Instruction Fetch*
- ID: *Instruction Decode*
- EXE: *Execution*
- MEM: *Memory*
- WB: *Write Back*

**Arquitectura sencilla y didáctica**

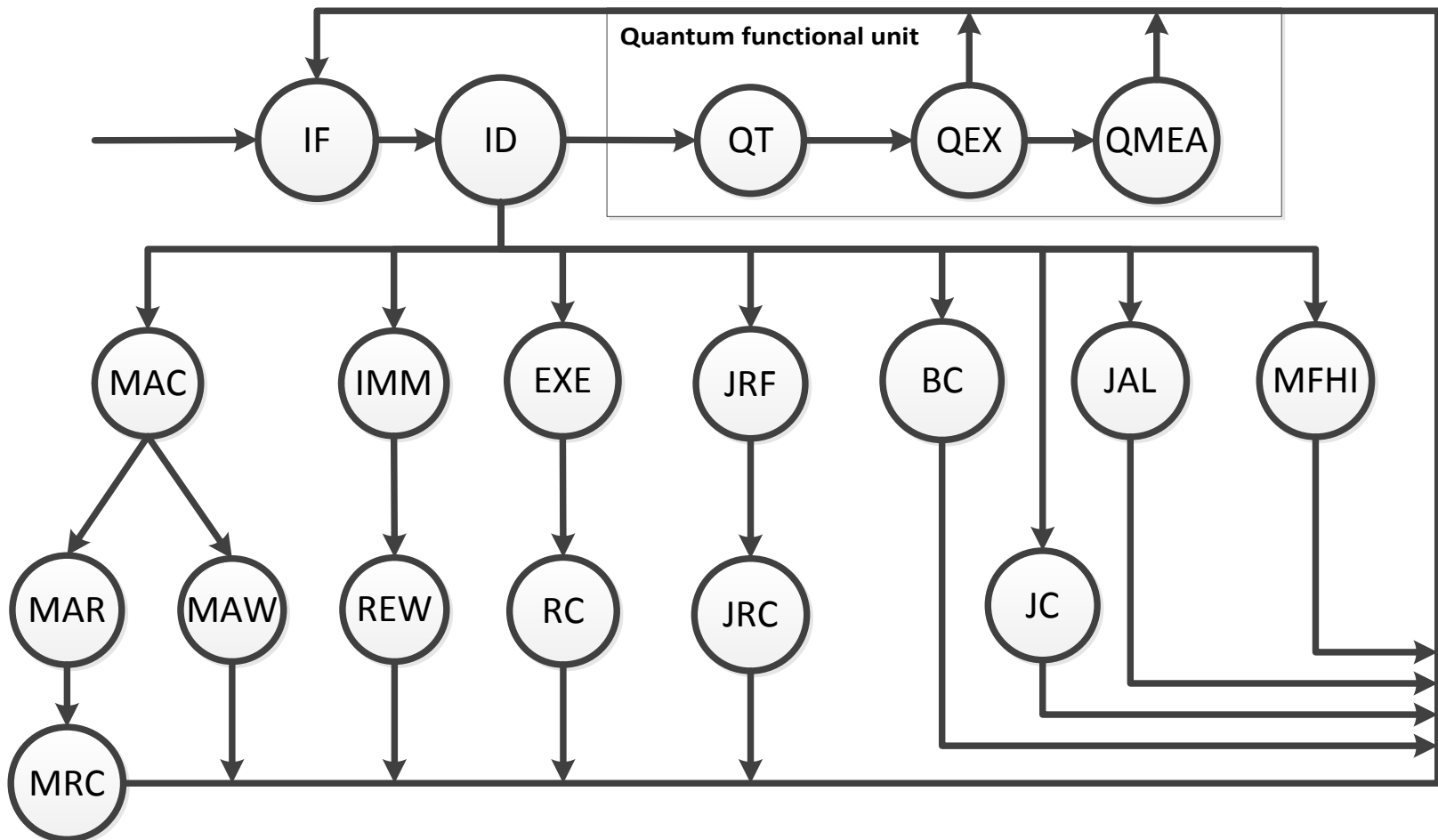
# Arquitectura qMIPS

## *Arquitectura simulada*



# Arquitectura qMIPS

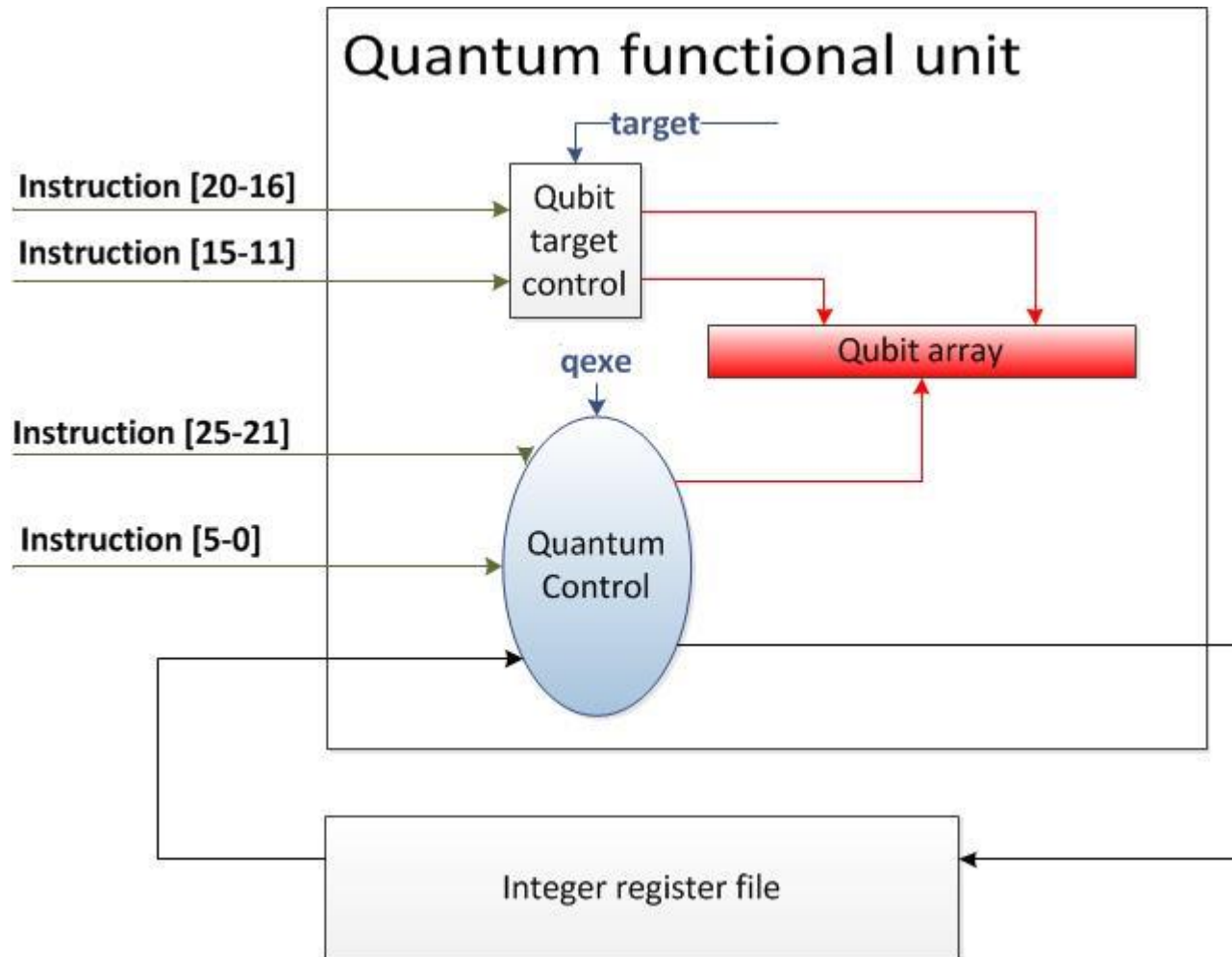
## *La unidad de control*





# Arquitectura qMIPS

## *La unidad funcional cuántica*







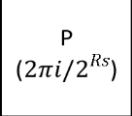
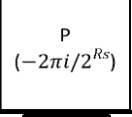

# Arquitectura qMIPS

## *Las instrucciones clásicas*

Instrucción	Resumen
add Rd, Rs, Rt	$Rd \leftarrow Rs + Rt$ (con desbordamiento)
addu Rd, Rs, Rt	$Rd \leftarrow Rs + Rt$ (sin desbordamiento)
sub Rd, Rs, Rt	$Rd \leftarrow Rs - Rt$ (con desbordamiento)
subu Rd, Rs, Rt	$Rd \leftarrow Rs - Rt$ (sin desbordamiento)
mult Rd, Rs, Rt	$Rd \leftarrow Rs \times Rt$ (bajos); $RHigh \leftarrow Rs \times Rt$ (altos)
div Rd, Rs, Rt	$Rd \leftarrow Rs / Rt$ (entera); $RHigh \leftarrow Rs / Rt$ (resto)
divu Rd, Rs, Rt	$Rd \leftarrow Rs / Rt$ (entera); $RHigh \leftarrow Rs / Rt$ (resto)
and Rd, Rs, Rt	$Rd \leftarrow Rs \text{ AND } Rt$
or Rd, Rs, Rt	$Rd \leftarrow Rs \text{ OR } Rt$
xor Rd, Rs, Rt	$Rd \leftarrow Rs \text{ XOR } Rt$
nor Rd, Rs, Rt	$Rd \leftarrow Rs \text{ NOR } Rt$
slt Rd, Rs, Rt	$Rd \leftarrow 1$ si $Rs > Rt$ ; sino $Rd \leftarrow 0$
addi Rd, Rs, C	$Rd \leftarrow Rs + C$ (con desbordamiento)
lw Rd, C(Rs)	$Rd \leftarrow \text{mem}[Rs + C]$
sw C(Rd), Rs	$\text{mem}[Rd + C] \leftarrow Rs$
jr Rs	$PC \leftarrow Rs$
j C (o etiqueta)	$PC \leftarrow C$
jal C (o etiqueta)	$R31 \leftarrow PC + 4$ ; $PC \leftarrow C$
beq Rs, Rt, C (o etiqueta)	$PC \leftarrow PC + C$ si $Rs = Rt$
bne Rs, Rt, C (o etiqueta)	$PC \leftarrow PC + C$ si $Rs \neq Rt$
trap C	Excepcion C
mfhi Rs	$Rs \leftarrow RHigh$

# Arquitectura qMIPS

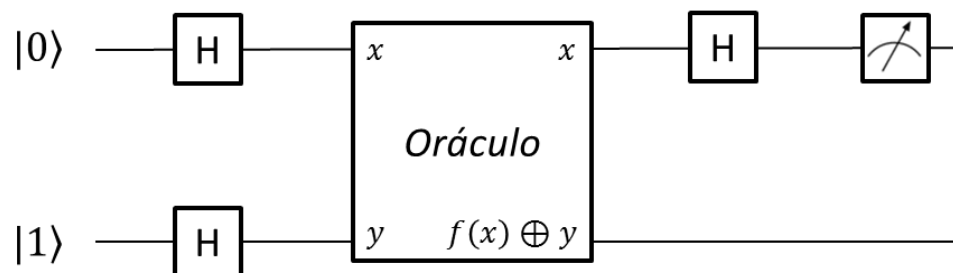
## *Las instrucciones cuánticas*

Instrucción	Resumen	Puerta
qhad Qt, Qc	Puerta de Hadamard.	
qx Qt, Qc	Puerta X de Pauli. Inversor.	
qy Qt, Qc	Puerta Y de Pauli.	
qz Qt, Qc	Puerta Z de Pauli.	
qphs Qt, Qc, Rs	Puerta $P(2\pi i/2^{Rs})$	
qnph Qt, Qc, Rs	Puerta $P(-2\pi i/2^{Rs})$	
qmea Qt, Rs, S	Rs <- Medida(Qt) desplazado Rs a la izquierda	
qrst Rs	Registro cuántico <- Rs	-

Instrucción	Resumen
qoff	Desplazamiento de etiquetas
qcnt	Selector de qubit de control

## 5

## El algoritmo de Deutsch



# El algoritmo de Deutsch

## *El problema de Deutsch*

Las cuatro funciones binarias de un bit

*Constante a 0:  $f(x) = 0$*

*Identidad:  $f(x) = x$*

*Constante a 1:  $f(x) = 1$*

*Negación:  $f(x) = \bar{x}$*

**Constantes**

**Equilibradas**

*“Dado un oráculo (o caja negra) que ejecuta una de las cuatro funciones binarias de un bit, decidir si esta es constante o equilibrada”*

# El algoritmo de Deutsch

## *Un intento clásico*

Se **llama al oráculo** mandándole un 0 como entrada.

Se obtiene una respuesta  $f(0) = a$

Como necesitamos más información **llamamos al oráculo** mandándole un 1

Se obtiene una respuesta  $f(1) = b$

Si  $a = b$  la función es constante y si  $a \neq b$  la función es equilibrada

**Son necesarias 2 llamadas al oráculo**

**El algoritmo cuántico lo consigue con tan solo una llamada**

# El algoritmo de Deutsch

## *Primer paso*

$$\left. \begin{array}{l}
 \text{Q0: } |0\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \Rightarrow \left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] \\
 \text{Q1: } |1\rangle \text{ --- } \boxed{\text{H}} \text{ --- } \Rightarrow \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]
 \end{array} \right\} \begin{array}{cc}
 \text{Q0} & \text{Q1} \\
 \left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] & \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]
 \end{array}$$

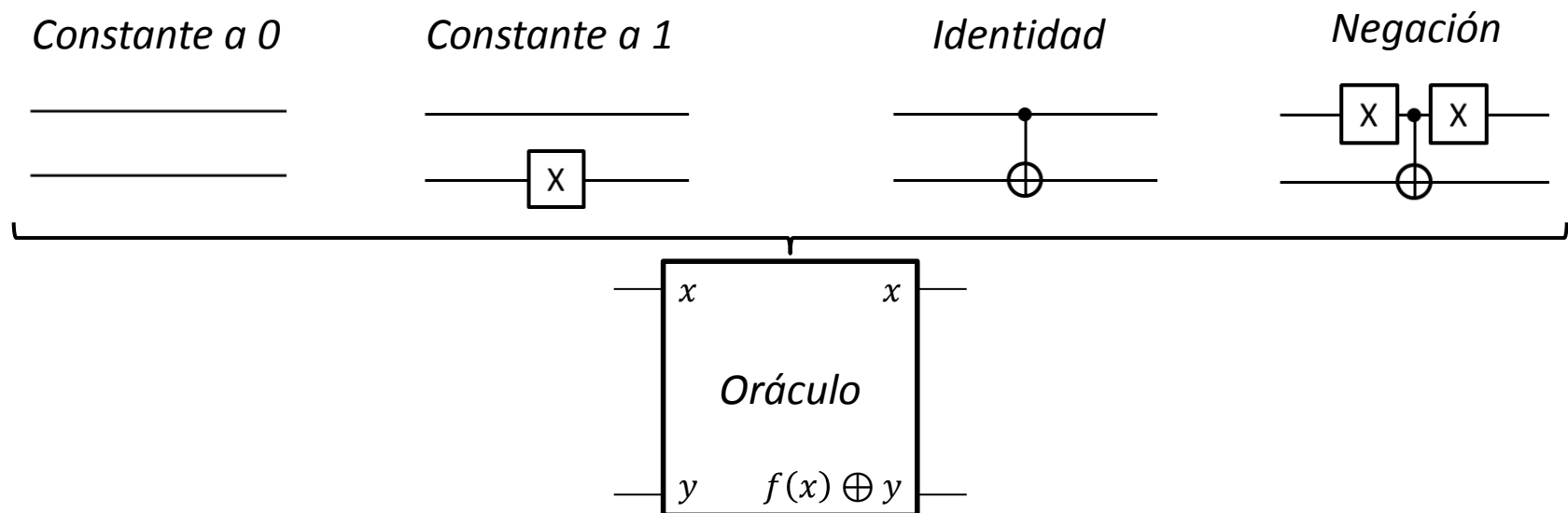
---


$$X \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] = \left[ \frac{1}{\sqrt{2}} (X|0\rangle - X|1\rangle) \right] = - \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right]$$

# El algoritmo de Deutsch

## *Segundo paso: el oráculo*

*“Si  $f(Q0)=1$  entonces niega  $Q1$ ”*



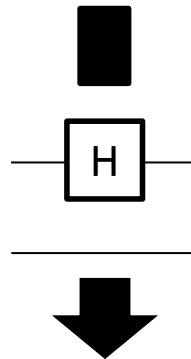
$$\begin{aligned}
 & \begin{array}{cc} \mathbf{Q0} & \mathbf{Q1} \\ \downarrow & \text{---} \end{array} \\
 & f\left(\frac{1}{2}|0\rangle(|0\rangle - |1\rangle)\right) + f\left(\frac{1}{2}|1\rangle(|0\rangle - |1\rangle)\right) = \\
 & \frac{1}{2}(-1)^{f(0)}|0\rangle(|0\rangle - |1\rangle) + \frac{1}{2}(-1)^{f(1)}|1\rangle(|0\rangle - |1\rangle)
 \end{aligned}$$



# El algoritmo de Deutsch

*Tercer paso: interferencia*

$$\begin{cases} \pm \left[ \frac{1}{\sqrt{2}} (|0\rangle + |1\rangle) \right] \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) = f(1) \\ \pm \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) \neq f(1) \end{cases}$$

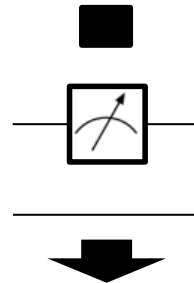


$$\begin{cases} \pm |0\rangle \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) = f(1) \\ \pm |1\rangle \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) \neq f(1) \end{cases}$$

# El algoritmo de Deutsch

*Último paso: medida*

$$\begin{cases} \pm |0\rangle \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) = f(1) \\ \pm |1\rangle \left[ \frac{1}{\sqrt{2}} (|0\rangle - |1\rangle) \right] & \text{si } f(0) \neq f(1) \end{cases}$$



**0** si el oráculo es constante

**1** si el oráculo es equilibrado

**Con tan solo una llamada al oráculo**

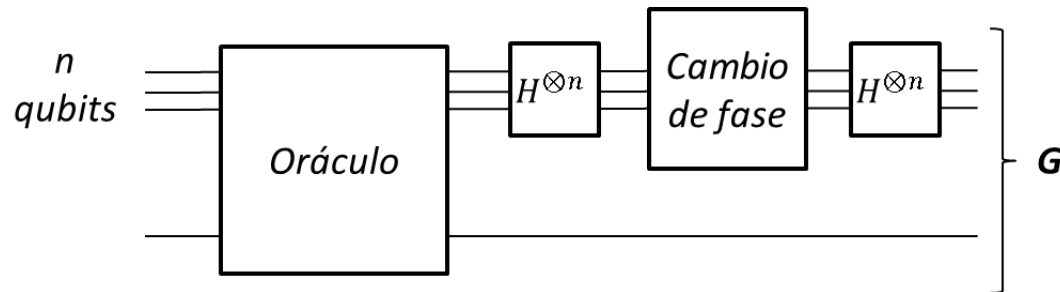
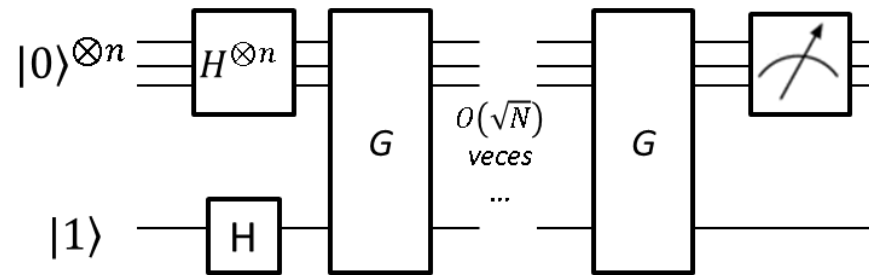
## 6

# El algoritmo de Grover



# El algoritmo de Grover

*El algoritmo de búsqueda*



Encuentra un dato en una lista desordenada en un tiempo  $O(\sqrt{N})$

7

# Conclusiones



# Conclusiones

## **qMIPS**

- Simulación de una arquitectura clásico-cuántica
- Versatilidad a la hora de programar
- Experimentación de la implementación física de los algoritmos
- Herramienta didáctica sobre computación cuántica

## **Qubit101**

- Simulación de circuitos cuánticos
- Facilidad para construir circuitos de alta complejidad
- Muy eficiente
- Banco de desarrollo y pruebas de algoritmos cuánticos



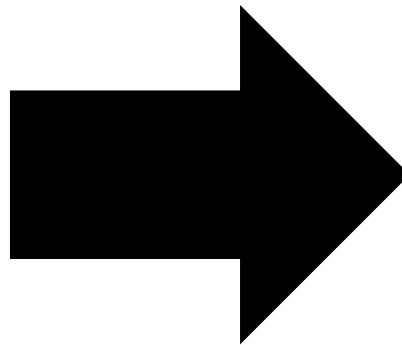
# Información cuántica

*¿Por qué un límite?*

Superposición de  
estados cuánticos

Entrelazamiento  
cuántico

Colapso de la  
función de onda



Paralelismo cuántico

Envío más rápido de  
información

Comunicaciones  
totalmente seguras

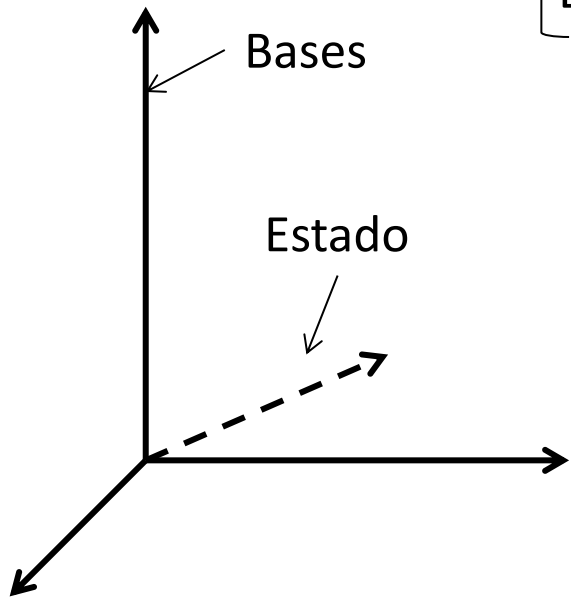


# Los postulados de la mecánica cuántica

## *Primer postulado: el espacio de estados*

Espacio de estados {

- Espacio vectorial complejo
- Producto interno definido (espacio de Hilbert)
- El vector de estado define completamente el sistema



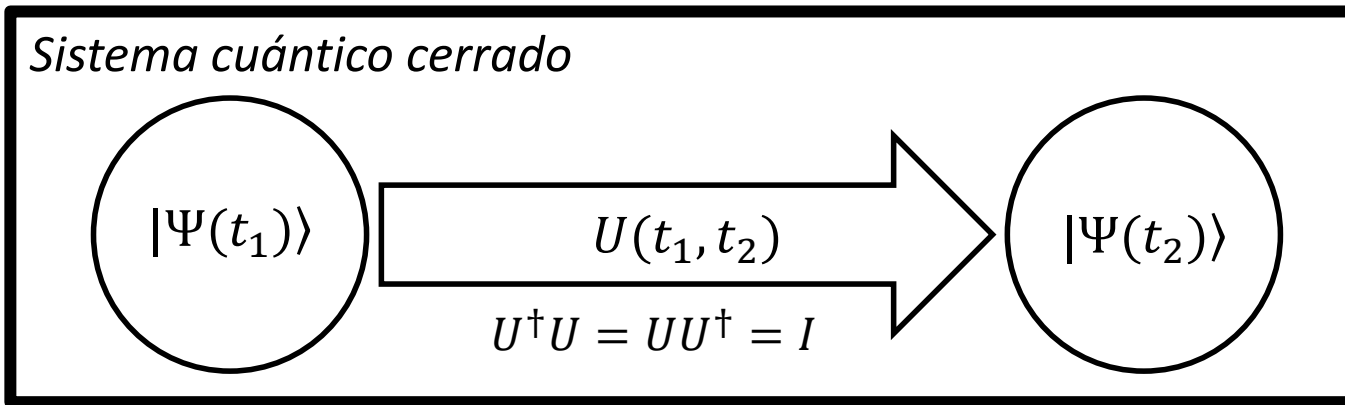
Estado arbitrario  
 $|\Psi\rangle$

Electrón orbitando un núcleo  
 $|n \ l \ m_l \ m_s\rangle$

Representación número de partículas  
 $|0 \ 2 \ 1 \ 4\rangle$

# Los postulados de la mecánica cuántica

*Segundo postulado: la evolución de los estados*



Podemos hacer evolucionar los estados a voluntad

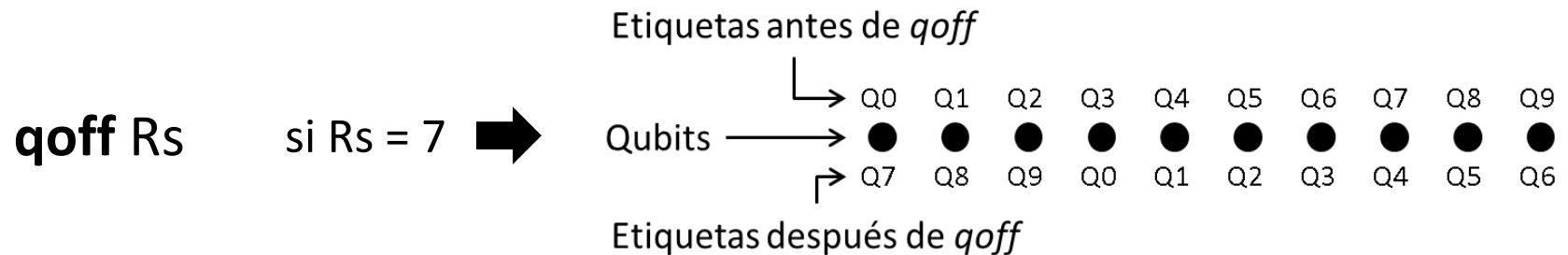
$$\text{Si } U^\dagger U = U U^\dagger = I \rightarrow U^{-1} = U^\dagger \quad \longrightarrow$$

Siempre existe operador inverso

**Las computaciones tienen  
que ser reversibles**

# Arquitectura qMIPS

## *Las instrucciones cuánticas de control*




---

**qcnt Rs**      ➡      si Rs = 5      ➡      Todas las puertas siguientes controladas por Q5